

Automatische certificaatschrijving en -verlenging configureren via CAPF Online CA

Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Achtergrondinformatie](#)
- [De servertijd en -datum valideren](#)
- [Computernaam bijwerken](#)
- [Configureren](#)
- [Advertentieservices, gebruikers- en certificaatsjabloon](#)
- [Configuratie van IIS-verificatie en SSL-binding](#)
- [CUCM-configuratie](#)
- [Verifiëren](#)
- [Controleer IIS-certificaten](#)
- [Controleer de CUCM-configuratie](#)
- [Verwante links](#)

Inleiding

Dit document beschrijft automatische certificaatschrijving en -verlenging via de online functie van de certificaatinstantie (CAPF) voor Cisco Unified Communications Manager (CUCM).

Bijgedragen door Michael Mendoza, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager
- X.509-certificaten
- Windows-server
- Windows Active Directory (AD)
- Windows Internet Information Services (IIS)
- NT (New Technology) LAN Manager (NTLM)-verificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM versie 12.5.1.10000-22
- Windows Server 2012 R2
- IP-telefoon CP-8865/firmware: SIP 12-1-1SR1-4 en 12-5-1SR2.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document behandelt de configuratie van het kenmerk en de bijbehorende bronnen voor aanvullend onderzoek.

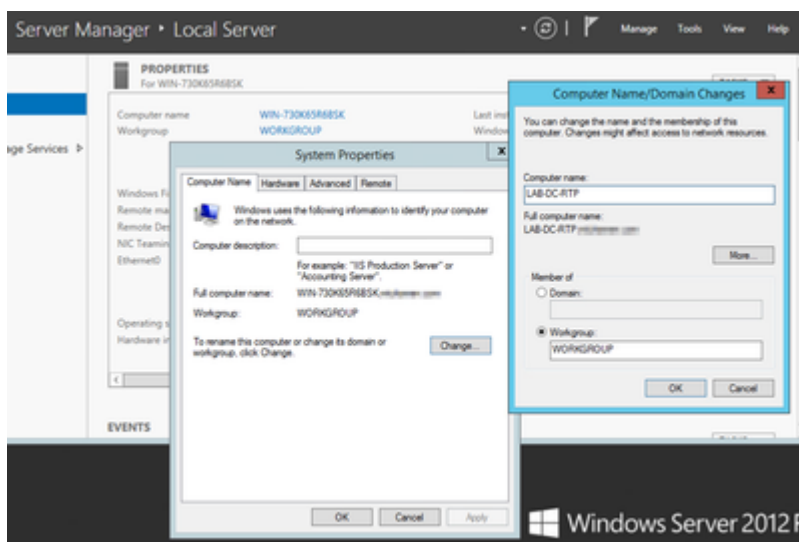
De servertijd en -datum valideren

Zorg ervoor dat de Windows-server de juiste datum, tijd en tijdzone heeft ingesteld, omdat dit van invloed is op de geldigheidstijden van het CA-certificaat (Certificate Authority) van de server en van de certificaten die door de server zijn afgegeven.

Computernaam bijwerken

Standaard heeft de computernaam van de server een willekeurige naam zoals WIN-730K65R6BSK. Het eerste wat moet worden gedaan voordat u AD Domain Services inschakelt, is ervoor te zorgen dat de computernaam van de server wordt bijgewerkt naar wat u wilt dat de hostnaam van de server en de hoofdnaam van de CA-uitgever aan het eind van de installatie zijn; anders duurt het veel extra stappen om dit te veranderen nadat AD-services zijn geïnstalleerd.

- Navigeer naar **lokale server** en selecteer de computernaam om de **steemeigenschappen** te openen
- Selecteer de knop **Wijzigen** en typ de nieuwe computernaam:



- Start de server opnieuw op om de wijzigingen te kunnen toepassen

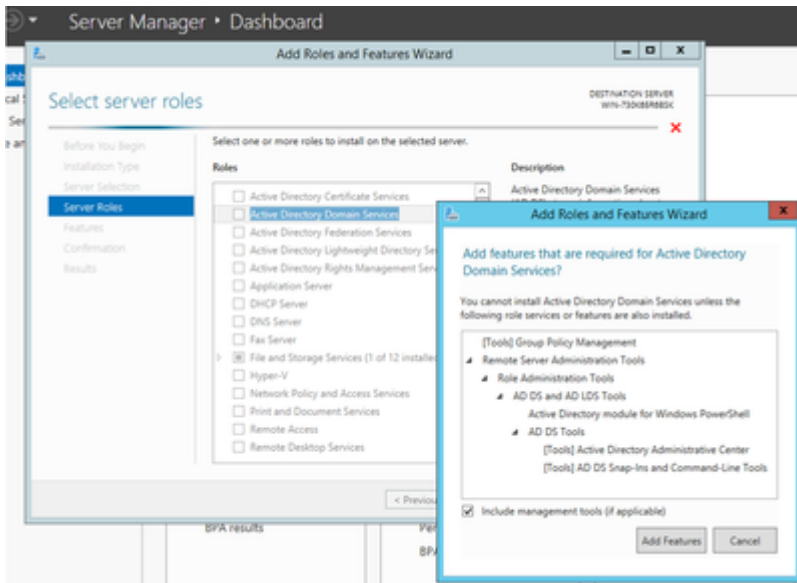
Configureren

Advertentieservices, gebruikers- en certificaatsjabloon

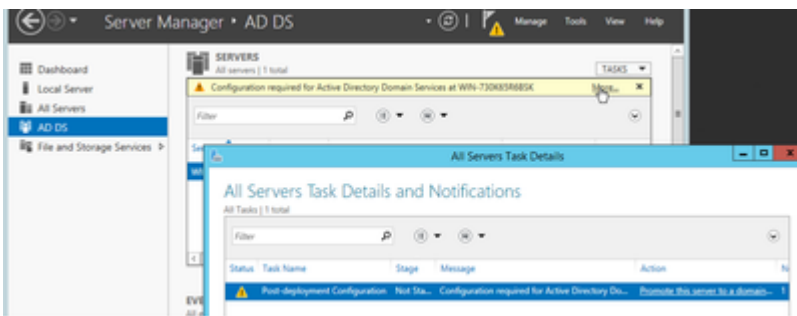
Active Directory-services inschakelen en configureren

- Selecteer in Server Manager de optie **Rollen en functies toevoegen**, selecteer **Role-based of feature-based installatie** en kies de server uit de pool (er moet er slechts één in de pool zijn) en vervolgens

Active Directory Domain Services:

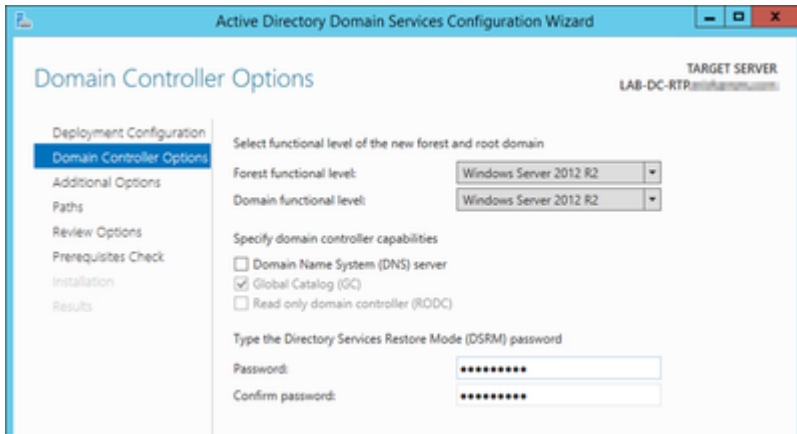


- Ga verder naar **Volgende** knop en vervolgens **Installeren**
- Selecteer de **sluitknop** nadat de installatie is voltooid
- Er verschijnt een waarschuwingstabblad onder **Server Manager > AD DS** met de titel Configuratie vereist voor Active Directory Domain Services; Selecteer **meer** koppeling en dan beschikbare actie om de setup-wizard te starten:

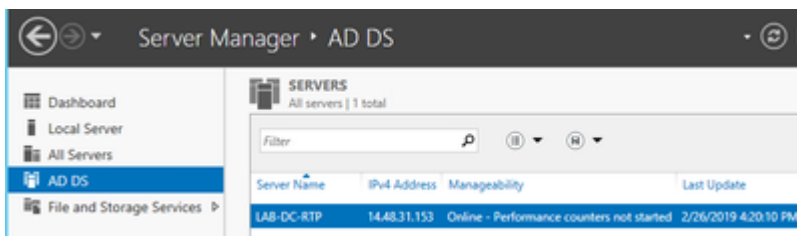


- Volg de aanwijzingen in de wizard Domeininstelling, voeg een nieuw Forest toe met de gewenste Root Domain Name (gebruikt michamen.com voor dit lab) en verwijder het DNS-vakje indien beschikbaar, definieer het DSRM-wachtwoord (gebruikt *C1sc0123!* voor dit lab):



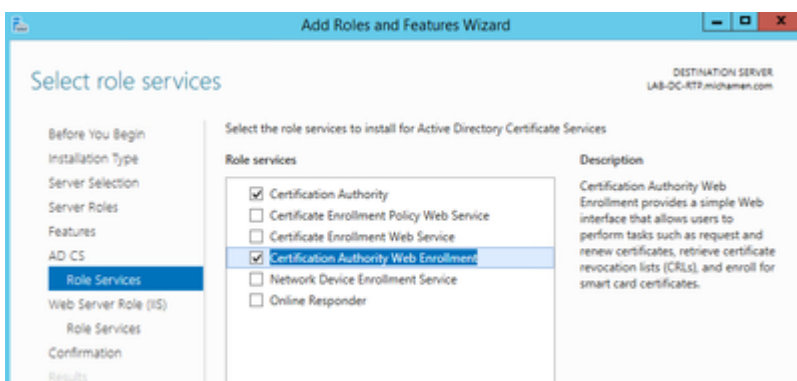


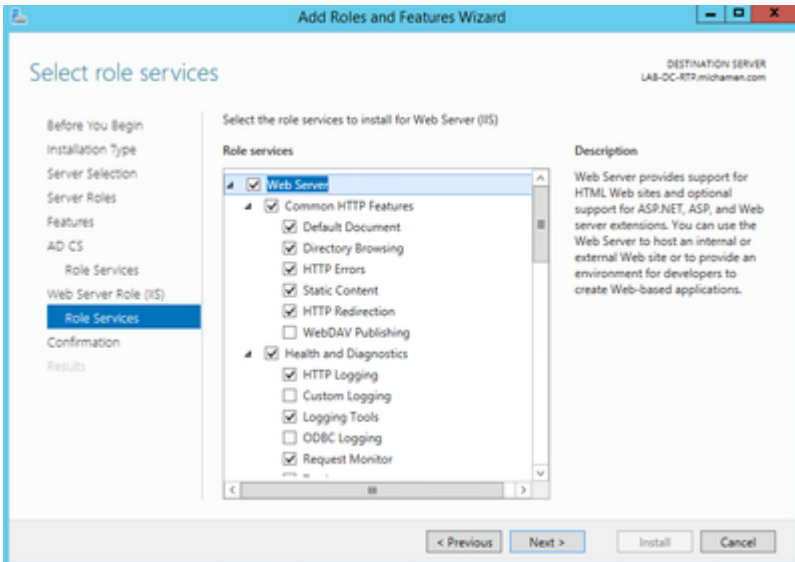
- Noodzaak om een NetBIOS domeinnaam te specificeren (gebruikt MICHAMEN1 in dit lab).
- Volg de wizard om dit te voltooien. Vervolgens start de server opnieuw op om de installatie te voltooien.
- Dan moet je de volgende keer dat je inlogt de nieuwe domeinnaam opgeven. Bijvoorbeeld MICHAMEN1\Administrator.



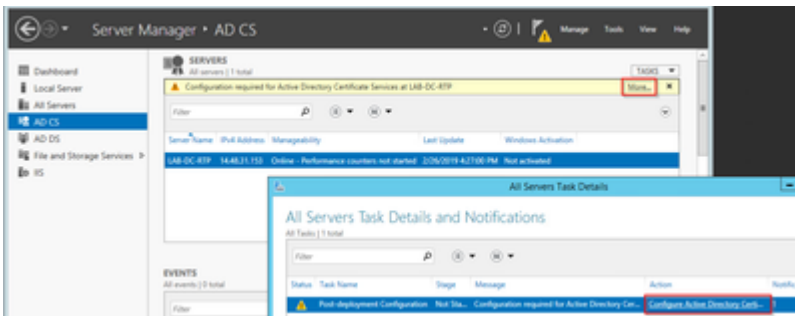
Certificatservices inschakelen en configureren

- Selecteer in Server Manager de optie Rollen en functies toevoegen
- Selecteer Active Directory-certificatservices en volg de aanwijzingen om de gewenste functies toe te voegen (alle beschikbare functies zijn geselecteerd uit de rolservices die voor dit lab zijn ingeschakeld)
- Voor webinschrijving voor Role Services controleer de certificeringsinstantie

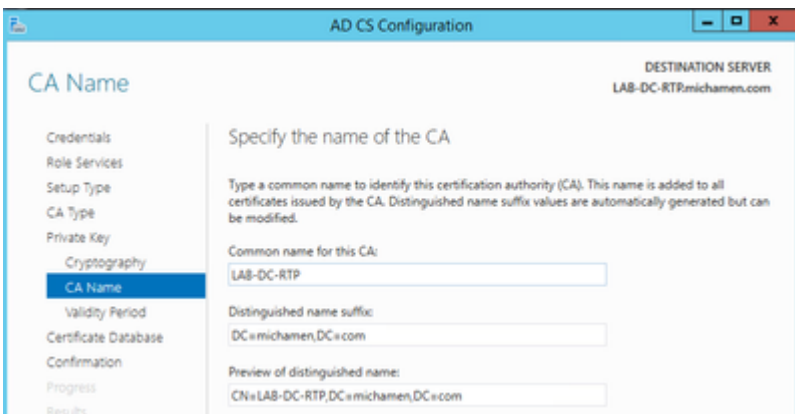




- Een waarschuwingstabblad moet verschijnen onder **Server Manager > AD DS** met de titel Configuratie vereist voor Active Directory Certificate Services; Selecteer de **meer** link en dan beschikbare actie:



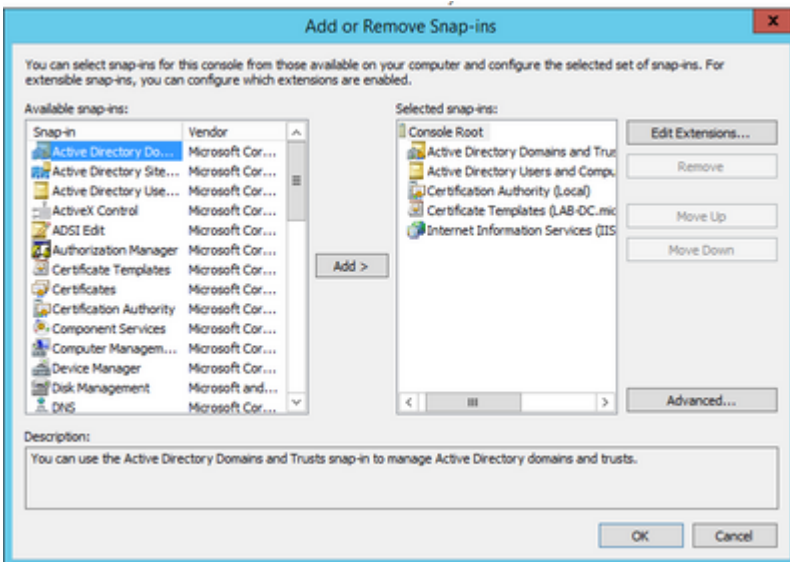
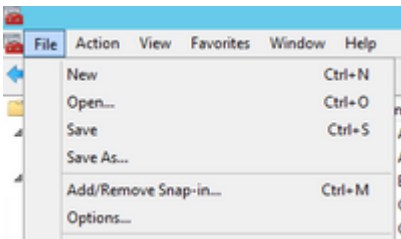
- Navigeer in de wizard Configuratie na installatie van AD-CS door de volgende stappen:
- Selecteer de **rollen** voor de **inschrijving van certificeringsinstanties** en **certificeringsinstanties**
- Kies Enterprise CA met opties:
- Root CA
- Een nieuwe privé-sleutel maken
- Private toets gebruiken - SHA1 met standaardinstellingen
- Stel een algemene naam in voor de CA (moet overeenkomen met de hostnaam van de server):



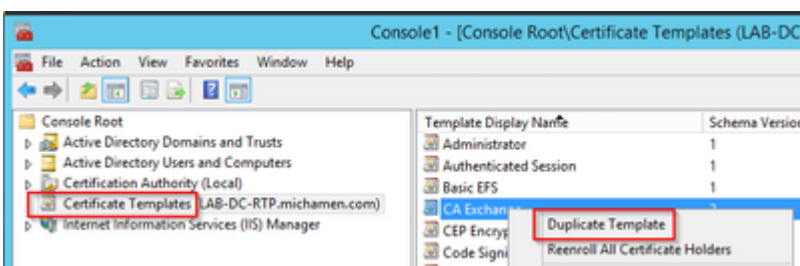
- Geldigheid instellen voor 5 jaar (of meer indien gewenst)
- Selecteer de knop **Volgende** door de rest van de wizard

Creatie van certificaatsjabloon voor CiscoRA

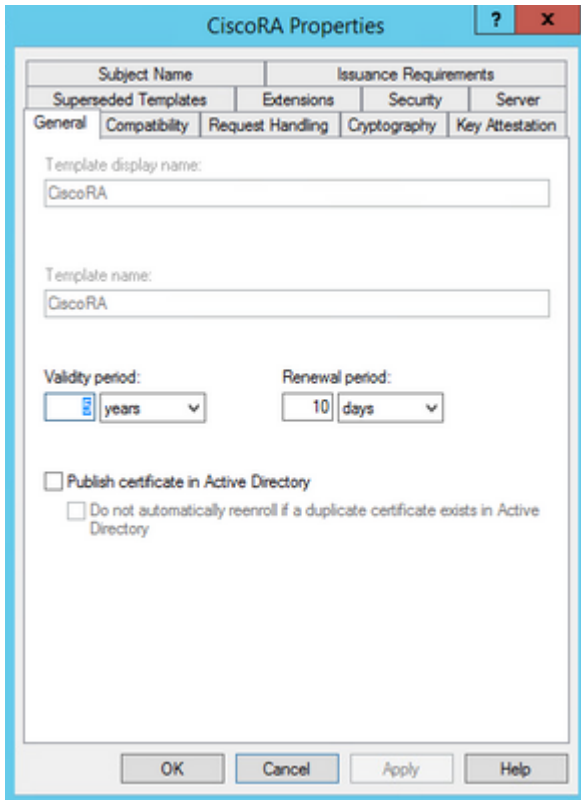
- Open MMC. Selecteer het Windows start logo en type *mmc* vanuit Run
- Open een MMC-venster en voeg de volgende snap-ins toe (gebruikt op verschillende punten van de configuratie) en selecteer vervolgens **OK**:



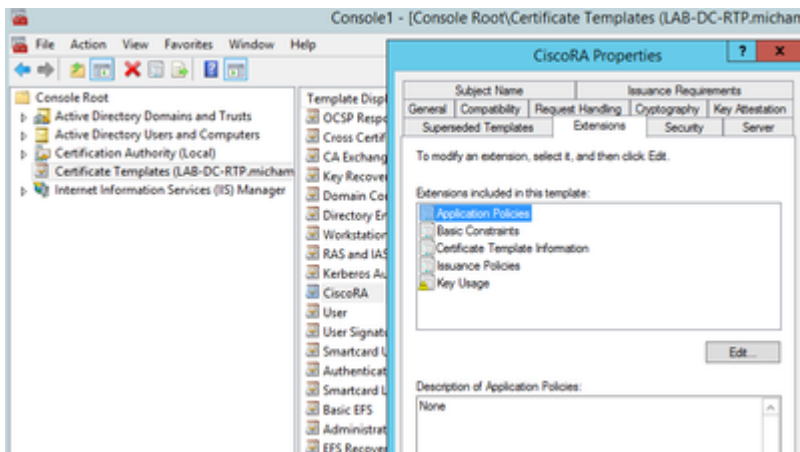
- Selecteer **Bestand** > Deze console sessie **opslaan** en opslaan op het bureaublad zodat u deze snel weer kunt openen
- Selecteer **certificaatsjablonen** in de invoegtoepassingen
- Maak of kloon een sjabloon (bij voorkeur de "*Root Certification Authority*"-sjabloon indien beschikbaar) en noem deze aan CiscoRA



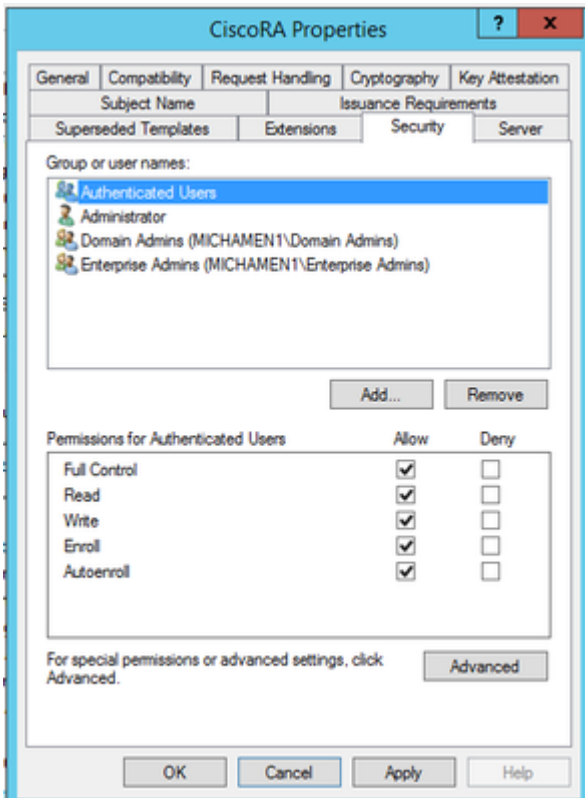
- Wijzig de sjabloon. Klik met de rechtermuisknop op de afbeelding en selecteer **Eigenschappen**
- Selecteer het tabblad **Algemeen** en stel de geldigheidsperiode in op 20 jaar (of een andere waarde indien gewenst). Zorg ervoor dat de "displaynaam" en "naam" van de sjabloon overeenkomen met deze tab



- Selecteer het tabblad **Extensies**, markeer **Toepassingsbeleid** en selecteer vervolgens **Bewerken**

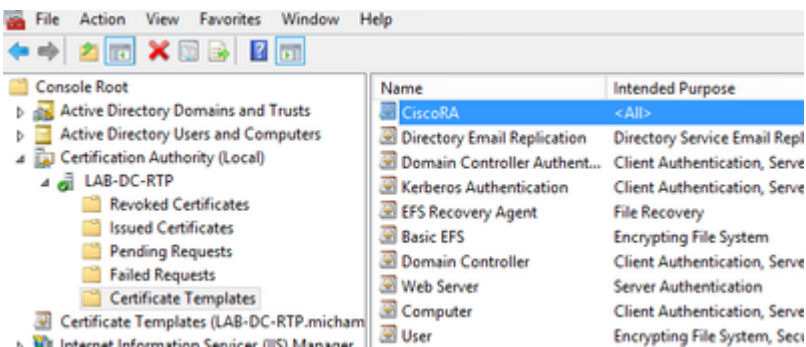


- Verwijder beleid dat is weergegeven in het venster dat wordt weergegeven
- Selecteer het tabblad **Onderwerpnaam** en selecteer de radioknop **Aanvragen**
- Selecteer het tabblad **Beveiliging** en geef alle rechten voor alle groepen/gebruikersnamen die worden weergegeven



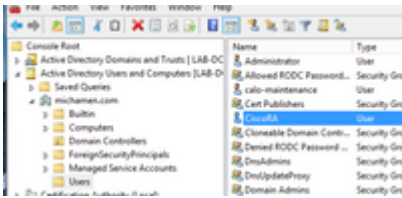
De certificaatsjabloon beschikbaar stellen voor afgifte

- Selecteer in de MMC-invoegtoepassing **Certificeringsinstantie** en vouw de mappenstructuur uit om de map **Certificaatsjablonen** te vinden
- Klik met de rechtermuisknop in de witte ruimte in het frame met de naam en het beoogde doel
- Selecteer **Nieuwe en te verstrekken certificaatsjabloon**
- De nieuwe Cisco RA-sjabloon selecteren en bewerken



Active Directory voor CiscoRA-account maken

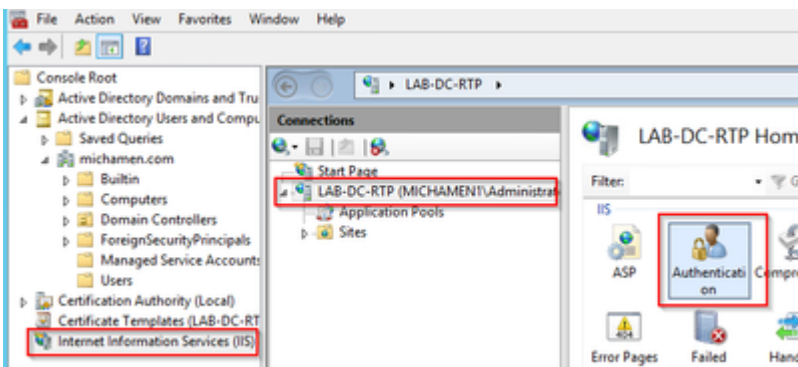
- Navigeren naar MMC snap-ins en selecteer **Active Directory-gebruikers en -computers**
- Selecteer de map **Gebruikers** in de structuur in het meest linkse deelvenster
- Klik met de rechtermuisknop in de witte ruimte in het frame met de naam, het type en de beschrijving
- Selecteer **Nieuw en Gebruiker**
- Maak de CiscoRA-account met gebruikersnaam/wachtwoord (*ciscora/Cisco123* is gebruikt voor dit lab) en selecteer het **selectievakje Wachtwoord** dat **nooit verloopt** wanneer dit wordt weergegeven



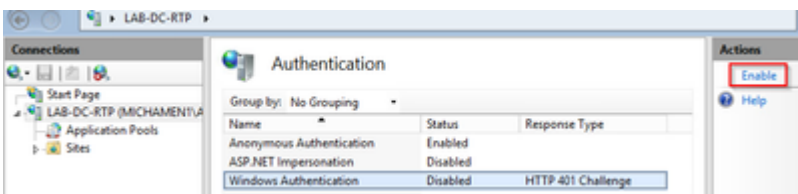
IIS Configuratie van verificatie en SSL-binding

Inschakelen NTLM Verificatie

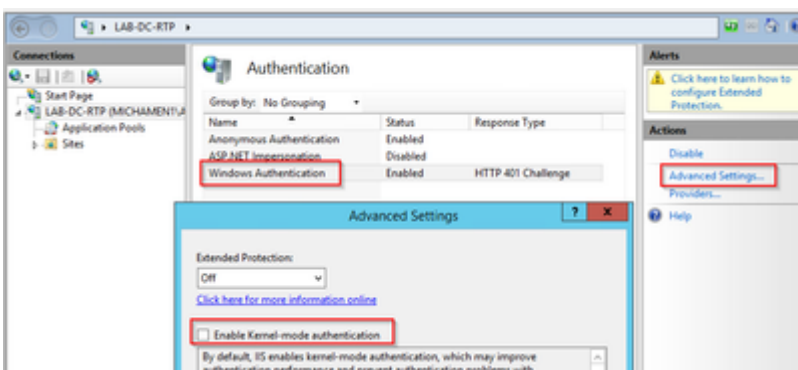
- Navigeer naar MMC snap-ins en selecteer de naam van uw server onder de Internet Information Services (IIS) Manager
- De lijst met functies wordt in het volgende frame weergegeven. Dubbelklik op het pictogram **van de verificatiefunctie**



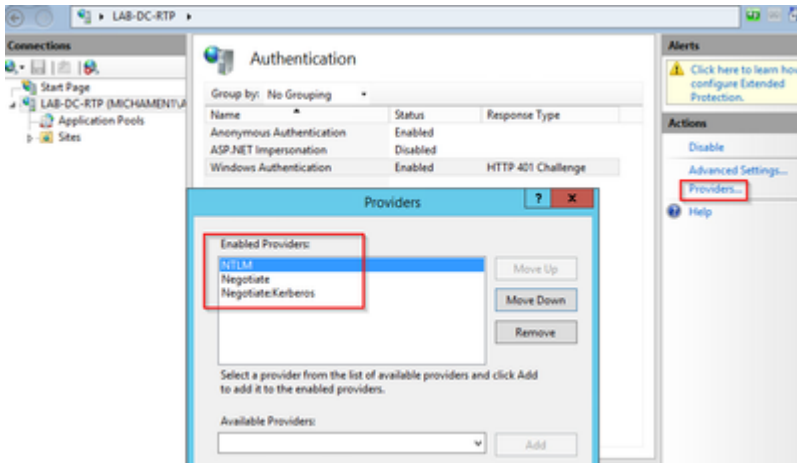
- Markeer **Windows-verificatie** en selecteer in het kader Handelingen (rechter deelvenster) de optie **Inschakelen**



- Het deelvenster Handelingen toont de optie **Geavanceerde instellingen**; selecteer deze optie en vink de optie **Kernel-mode-verificatie inschakelen uit**



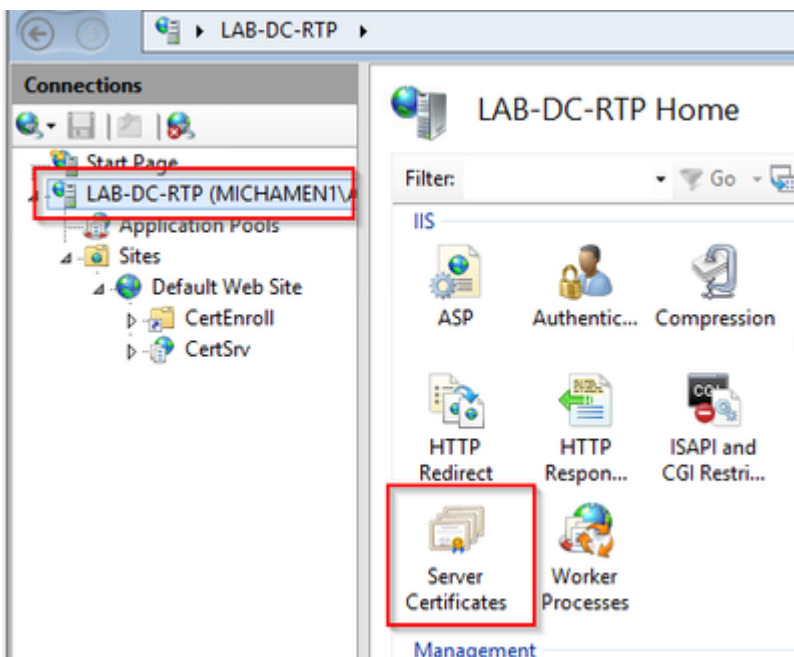
- Selecteer **Providers** en zet orde in **NTML** dan **Onderhandelen**.



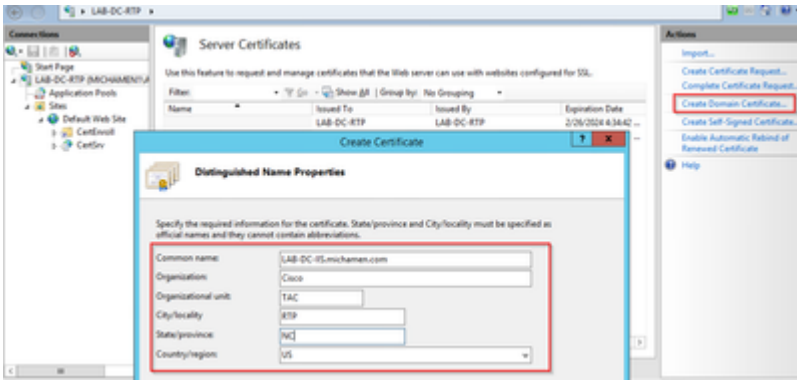
Het identiteitscertificaat voor de webserver genereren

Als dat nog niet het geval is, moet u een certificaat en een identiteitscertificaat voor uw webservice genereren dat door de CA is ondertekend, omdat CiscoRA geen verbinding met de case kan maken als het certificaat van de webserver zelfondertekend is:

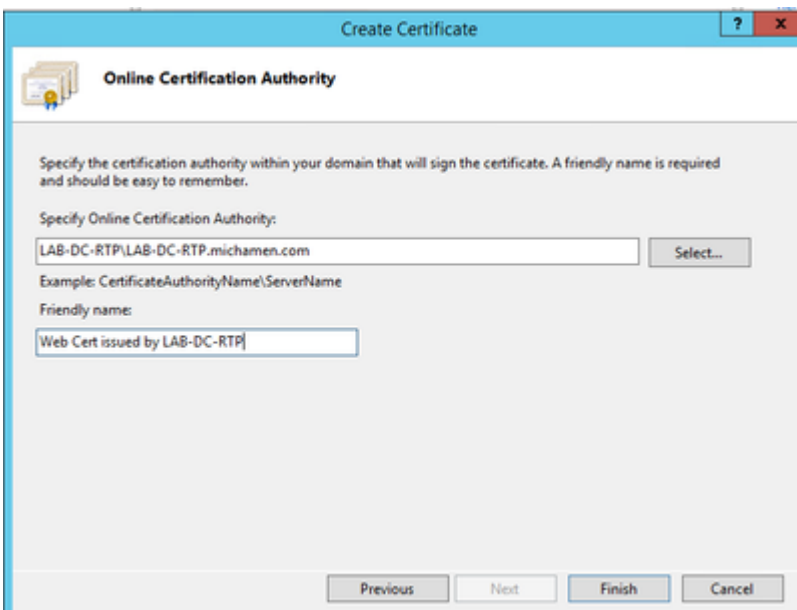
- Selecteer uw webserver **onverwacht-in** van **IIS** en dubbelklik op het functiepictogram **Server Certificates**:



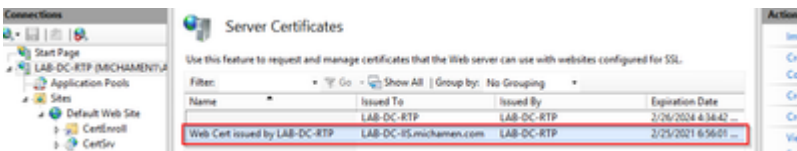
- Standaard kunt u één certificaat zien dat daar wordt vermeld; dat is de zelfondertekende root-CA-cert; In het menu **Acties** selecteert u de optie **Domeincertificaat maken**. Voer de waarden in van de configuratiewizard om uw nieuwe certificaat te maken. Zorg ervoor dat de algemene naam een oplosbare FQDN is (volledig gekwalificeerde domeinnaam) en selecteer vervolgens **Volgende**:



- Selecteer het basiscertificaat van uw CA om de emittent te zijn en selecteer **Voltoeien**:

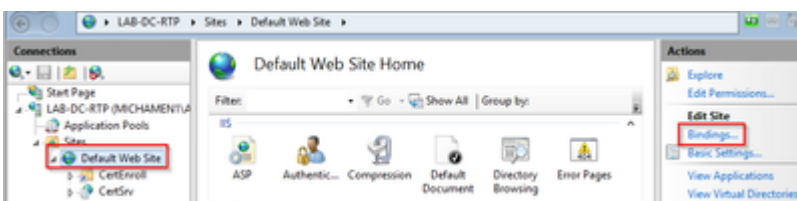


- U kunt beide zien, het CA-certificaat en het identiteitscertificaat van uw webserver:

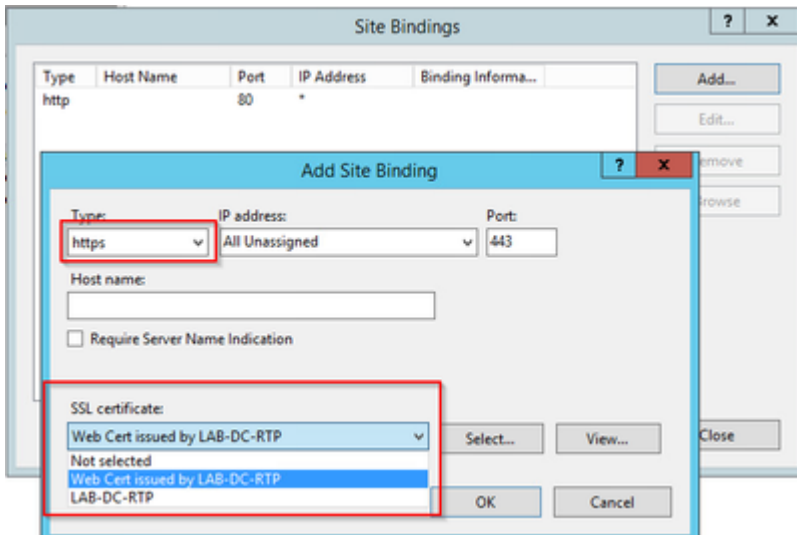


SSL-binding voor webservers

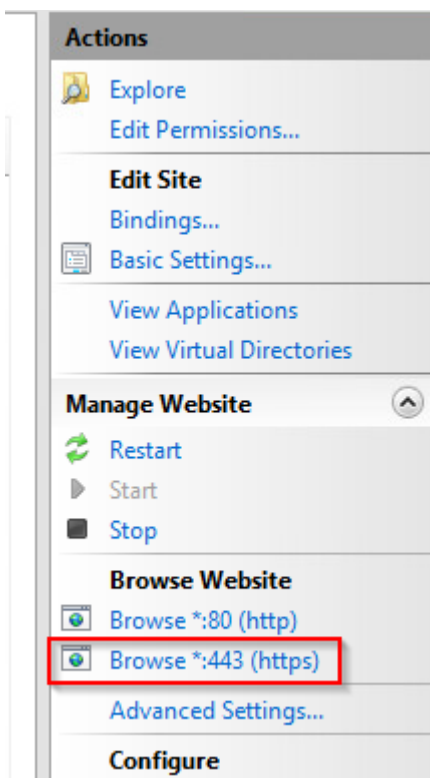
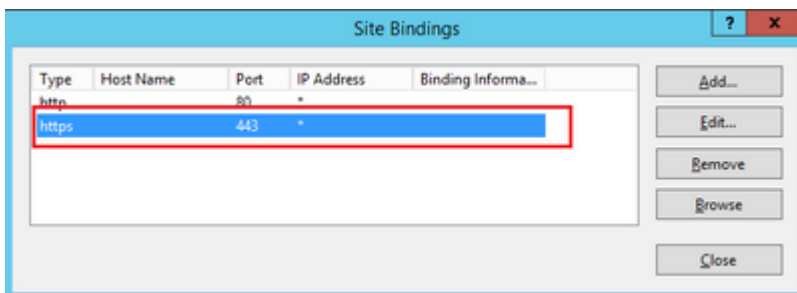
- Selecteer een site in de boomstructuur weergave (u kunt de Standaardwebsite gebruiken of deze verfijnder maken voor specifieke sites) en selecteer **Bindingen** in het deelvenster Handelingen. Dit brengt de bindingen editor die u in staat stelt om bindingen voor uw website te maken, bewerken en verwijderen. Selecteer **Add** om uw nieuwe SSL-band aan de site toe te voegen.



- De standaardinstellingen voor een nieuwe binding worden op HTTP op poort 80 ingesteld. Selecteer **https** in de vervolgkeuzelijst **Type**. Selecteer het zelfondertekende certificaat dat u in de vorige sectie hebt gemaakt in de vervolgkeuzelijst **SSL-certificaat** en selecteer vervolgens **OK**.



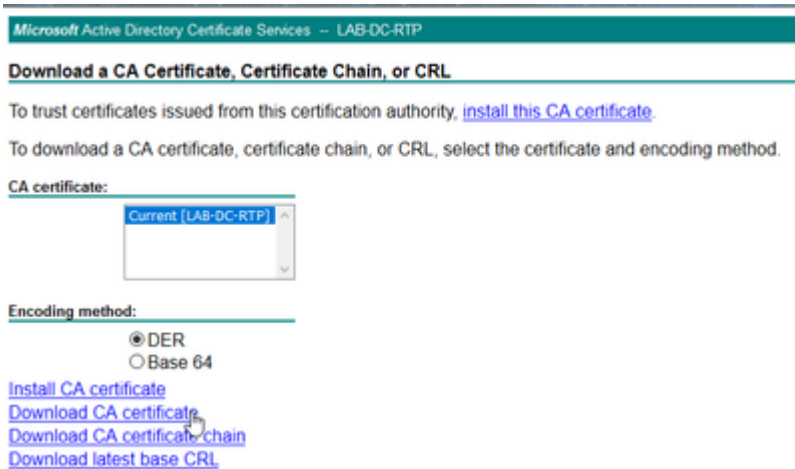
- Nu hebt u een nieuwe SSL-binding op uw site en alles wat overblijft is te verifiëren dat het werkt door te selecteren **Bladeren *:443 (https)** optie uit het menu en ervoor te zorgen dat de standaard IIS-webpagina gebruik maakt van HTTPS:



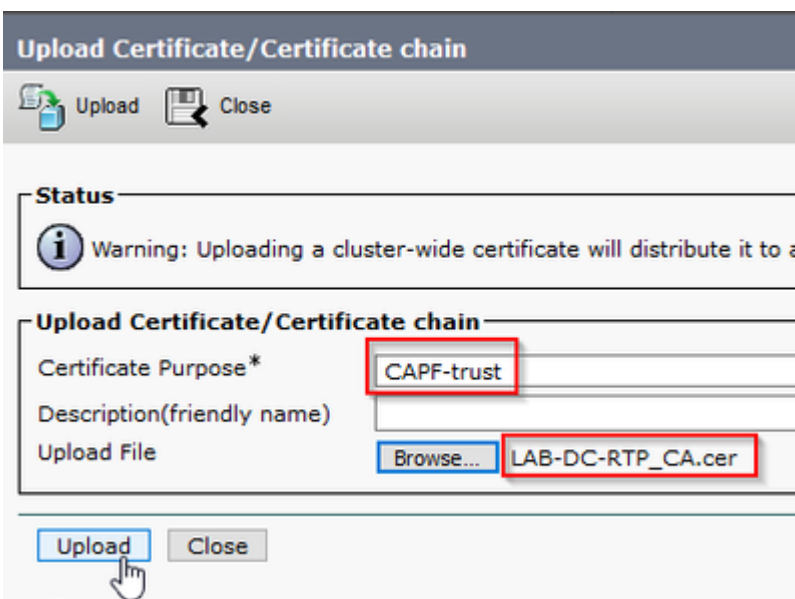
- Herinner me om de dienst opnieuw te beginnen IIS na configuratieveranderingen. Gebruik de optie **Opnieuw starten** in het deelvenster Handelingen.

CUCM-configuratie

- Navigeer naar uw AD CS-webpagina (https://YOUR_SERVER_FQDN/certsrv/) en download het CA-certificaat



- Navigeer naar **Security > Certificate Management** vanaf de beheerpagina van het besturingssysteem en selecteer de knop **Upload Certificate/Certificate** om het CA-certificaat te uploaden met het *doel dat is* ingesteld op *CAPF-trust*.



... Op dit punt is het ook een goed idee om dat zelfde certificaat van CA als *CallManager-trust* te uploaden omdat het nodig is als de veilige signaleringsencryptie voor de eindpunten wordt toegelaten (of zal worden toegelaten); wat waarschijnlijk is als het cluster in Gemengde modus is.

- Ga naar **Systeem > Serviceparameters**. Selecteer de Unified CM Publisher-server in het serverveld en de **Cisco Certificate Authority Proxy-functie** in het veld Service
- Stel de waarde van Certificaatverlener in op Endpoint naar Online CA en voer de waarden in voor de velden Online CA-parameters. Zorg ervoor dat u de FQDN van de webserver gebruikt, de naam van de certificaatsjabloon die eerder is gemaakt (CiscoRA), het CA-type als Microsoft CA en gebruik de referenties van de CiscoRA-gebruikersaccount die eerder is gemaakt

Service Parameter Configuration

 Save  Set to Default

Select Server and Service

Server*
 Service*

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Cisco Certificate Authority Proxy Function (Active) Parameters on server cucm125pub--CUCM Voice/Video (Active)

Parameter Name	Parameter Value
Certificate Issuer to Endpoint *	Online CA
Duration Of Certificate Validity (in days) *	1825
Key Size *	1024
Maximum Allowable Time For Key Generation *	30
Maximum Allowable Attempts for Key Generation *	3

Online CA Parameters

Online CA Hostname	lab-dc-iis.michamen.com
Online CA Port	443
Online CA Template	CiscoRA
Online CA Type *	Microsoft CA
Online CA Username	••••••••
Online CA Password	••••••••

- In een pop-venster wordt aangegeven dat de CAPF-service opnieuw moet worden gestart. Maar activeer eerst de Cisco-service voor certificaatschrijving via **Cisco Unified Service > Tools > Serviceactivering**, selecteer de uitgever in het veld Server en controleer het selectievakje Cisco Certificate Enrollment Service (Cisco-certificaatschrijvingservice) en selecteer vervolgens de knop **Opslaan**:

Service Name	Activation Status
<input checked="" type="checkbox"/> Cisco Certificate Authority Proxy Function	Activated
<input checked="" type="checkbox"/> Cisco Certificate Enrollment Service	Deactivated
<input checked="" type="checkbox"/> Cisco CTL Provider	Activated

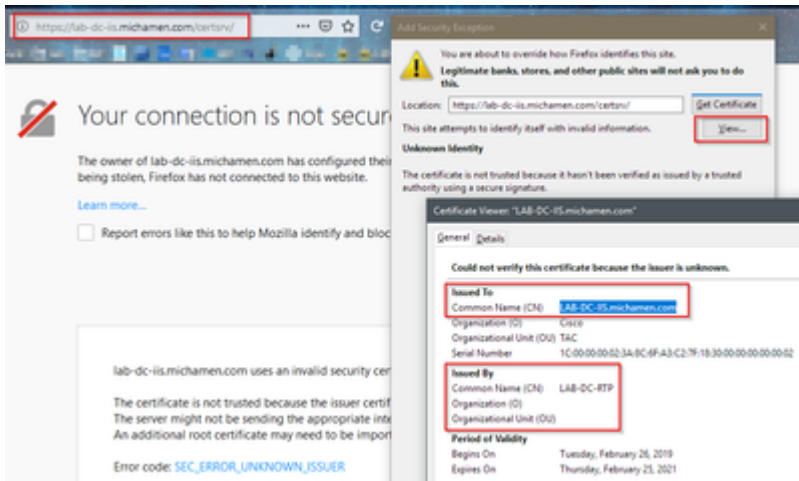
Verifiëren

Controleer IIS-certificaten

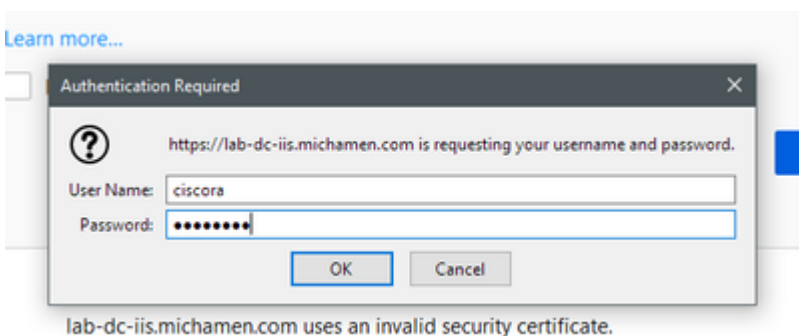
- Van een browser van het Web in een PC met connectiviteit aan de server (bij voorkeur in het zelfde netwerk zoals de Uitgever CUCM) navigeer aan URL:

https://YOUR_SERVER_FQDN/certsrv/

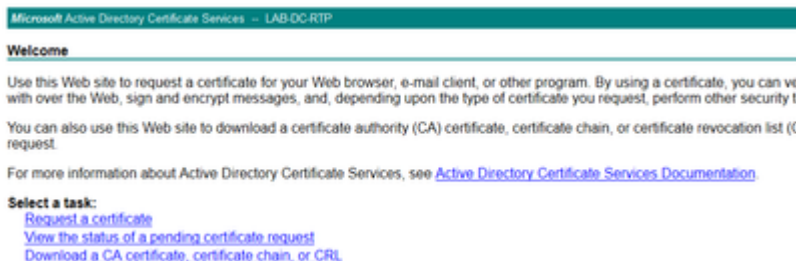
- Er wordt een waarschuwing weergegeven dat het certificaat niet betrouwbaar is. Voeg de uitzondering toe en controleer het certificaat. Zorg ervoor dat deze overeenkomt met de verwachte FQDN:



- Nadat u de uitzondering hebt geaccepteerd, dient u te verifiëren; op dit punt dient u de aanmeldingsgegevens te gebruiken die eerder voor de CiscoRA-account zijn geconfigureerd:



- Na verificatie moet u de AD CS (Active Directory Certificate Services) welkomspagina kunnen zien:



Controleer de CUCM-configuratie

Voer de stappen uit die u normaal volgt om een LSC-certificaat op een van de telefoons te installeren.

Stap 1. Open de pagina CallManager-beheer, het apparaat en vervolgens de telefoon

Stap 2. Selecteer de knop **Zoeken** om de telefoons weer te geven

Stap 3. Selecteer de telefoon waarop u de LSC wilt installeren

Stap 4. Blader naar beneden naar informatie over de certificeringsinstantie-proxyfunctie (CAPF)

Stap 5. Selecteer de optie Installeren/upgraden vanuit de werking van het certificaat.

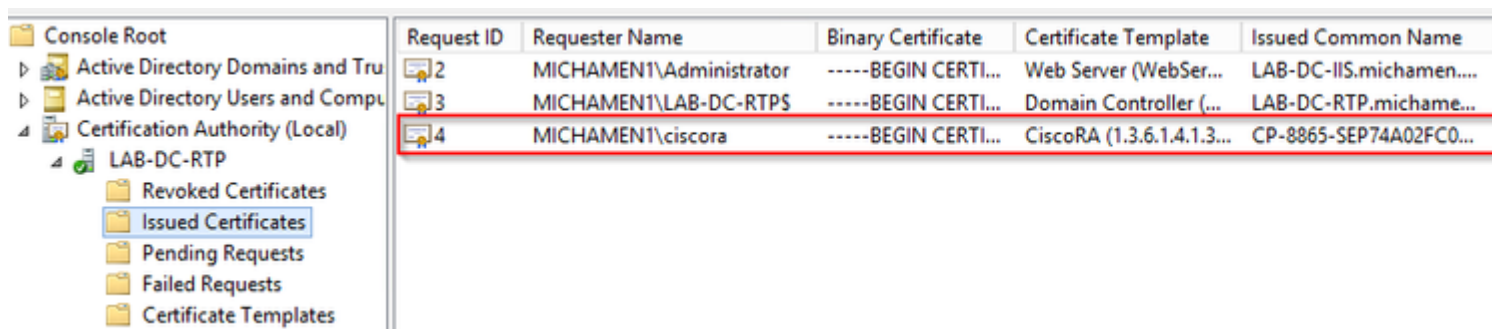
Stap 6. Selecteer de Verificatiemodus. (Bij Null String is geen probleem voor testdoeleinden)

Stap 7. Schuif naar de bovenkant van de pagina en selecteer **opslaan** en **pas** vervolgens **Config toe** op de

telefoon.

Stap 8. Nadat de telefoon herstart en opnieuw registreert, gebruikt u het filter LSC Status om te bevestigen dat de LSC met succes is geïnstalleerd.

- Open MMC van de AD-server en vouw de invoegtoepassing Certificeringsinstantie uit om de map Afgegeven certificaten te selecteren
- De ingang voor de telefoon wordt getoond Binnen de summere mening, zijn dit enkele getoonde details:
 - Aanvraag-ID: uniek volgnummer
 - Naam aanvrager: de gebruikersnaam voor de geconfigureerde CiscoRA-account moet worden weergegeven
 - Certificaatsjabloon: de naam van de gemaakte CiscoRA-sjabloon moet worden weergegeven
 - Uitgegeven gemeenschappelijke naam: Het model van de telefoon dat door de apparatenaam wordt toegevoegd moet worden getoond
 - Effectieve datum en vervaldatum certificaat



Request ID	Requester Name	Binary Certificate	Certificate Template	Issued Common Name
2	MICHAMEN1\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	LAB-DC-IIS.michamen...
3	MICHAMEN1\LAB-DC-RTPS	-----BEGIN CERTI...	Domain Controller (...	LAB-DC-RTP.michame...
4	MICHAMEN1\ciscora	-----BEGIN CERTI...	CiscoRA (1.3.6.1.4.1.3...	CP-8865-SEP74A02FC0...

Verwante links

- [CAPF Online CA voor probleemoplossing](#)
- [Technische ondersteuning en documentatie â€™ Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.